IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Arvind Ramaswamy et al.	§	Confirmation No.:	6801
Serial No.:	10/506,815	§	Group Art Unit:	2446
Filed:	04/11/2005	§	Examiner:	Farhad Ali
For:	Method And System For A Network Management Console	§	Docket No.:	200601202-5

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: June 21, 2010

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on April 20, 2010.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventors to Peregrine Systems, Inc., was recorded on December 12, 2005, at Reel/Frame 017328/0356. The Merger document from Peregrine Systems, Inc. to HPC was recorded on May 31, 2006, at Reel/Frame 017703/0668. The Assignment from HPC to HPDC was recorded on July 10, 2006, at Reel/Frame 017905/0174.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-19.
Claim cancellations:	None.
Added claim:	20.
Presently pending claims:	1-20.
Presently appealed claims:	1-20.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the Office Action dated January 21, 2010.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellants. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

1. A data network management system for identifying unauthorized access to a data network service,[1] provided at a service node in a data network,[2] by a user node in said data network,[3] said service node having an agent[4] and having means for maintaining a user access list,[5] said user access list having at least one data network address corresponding to at least one user node in said data network,[6] said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said service node;[7]

---

[1] Fig. 1 (110). Disclosure p. 10, lines 1-4 of paragraph [0029].

[2] Fig. 1 (230, 260, 300). Disclosure p. 13, lines 2-4 of paragraph [0035].

[3] Fig. 1 (200, 210, 240, 250, 270, 280). Disclosure p. 12, lines 16-20 of paragraph [0032].

[4] Fig. 1 (230, 260, 300). Disclosure p. 12-13, lines 4-13 of paragraph [0034].

[5] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[6] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[7] Fig. 1 (110). Disclosure p. 14, lines 3-11 of paragraph [0037].

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node;[8] and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.[9]

5. A method for identifying unauthorized access to a data network service, provided at a service node in a data network,[10] by a user node in said data network,[11] said service node having an agent[12] and having means for maintaining a user access list,[13] said user access list having at least one data network address corresponding to at least one user node in said data network,[14] said method comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network;[15]

b) comparing said user access list to an authorized access list;[16]

c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list;[17] and

---

[8] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[9] Fig. 1 (110). Disclosure p. 14-15, lines 1-15 of paragraph [0038].

[10] Fig. 1 (230, 260, 300). Disclosure p. 13, lines 2-4 of paragraph [0035].

[11] Fig. 1 (200, 210, 240, 250, 270, 280). Disclosure p. 12, lines 16-20 of paragraph [0032].

[12] Fig. 1 (230, 260, 300). Disclosure p. 12-13, lines 4-13 of paragraph [0034].

[13] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[14] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[15] Fig. 3 (470, 480). Disclosure p. 17, lines 5-10 and 15-17 of paragraph [0043].

[16] Fig. 3 (490). Disclosure p. 18, lines 17-19 of paragraph [0043].

[17] Fig. 3 (500). Disclosure p. 18, lines 19-21 of paragraph [0043].

d) if said access was not authorized, initiating a notification process;[18]

wherein said user access list identifies a plurality of accesses to said service node.[19]

13. A computer-readable medium for identifying unauthorized access to a data network service, provided at a service node in a data network,[20] by a user node in said data network,[21] said service node having an agent[22] and having means for maintaining a user access list,[23] said user access list having at least one data network address corresponding to at least one user node in said data network,[24] and said medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor, cause said processor to perform steps comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in a data network;[25]

b) comparing said user access list to an authorized access list;[26]

c) determining if an access to said data network service was authorized based on said comparison step b);[27]

d) if determined that said access was unauthorized, initiating a notification process.[28]

---

[18] Fig. 3 (520). Disclosure p. 18, lines 23-28 of paragraph [0043].

[19] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[20] Fig. 1 (230, 260, 300). Disclosure p. 13, lines 2-4 of paragraph [0035].

[21] Fig. 1 (200, 210, 240, 250, 270, 280). Disclosure p. 12, lines 16-20 of paragraph [0032].

[22] Fig. 1 (230, 260, 300). Disclosure p. 12-13, lines 4-13 of paragraph [0034].

[23] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[24] Fig. 1 (230, 260, 300). Disclosure p. 14, lines 12-15 of paragraph [0036].

[25] Fig. 3 (470, 480). Disclosure p. 17, lines 5-10 and 15-17 of paragraph [0043].

[26] Fig. 3 (490). Disclosure p. 18, lines 17-19 of paragraph [0043].

[27] Fig. 3 (500). Disclosure p. 18, lines 19-21 of paragraph [0043].

[28] Fig. 3 (520). Disclosure p. 18, lines 23-28 of paragraph [0043].

18. A computer for use in a data network for identifying unauthorized access to a data network service,[29] provided at a service node in a data network,[30] by a user node in said data network,[31] said service node having an agent[32] and having means for maintaining a user access list,[33] said user access list having at least one data network address corresponding to at least one user node in said data network;[34] said computer comprising:

means for storing an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node;[35]

a central processing unit;[36]

data communication means for periodically polling said agent at said service node and retrieving a user access list from said agent, said user access list specifying which users have accessed said service node;[37] and

data processing means for comparing said retrieved user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.[38]

---

[29] Fig. 1 (110). Disclosure p. 10, lines 1-4 of paragraph [0029].

[30] Fig. 1 (230, 260, 300). Disclosure p. 13, lines 2-4 of paragraph [0035].

[31] Fig. 1 (200, 210, 240, 250, 270, 280). Disclosure p. 12, lines 16-20 of paragraph [0032].

[32] Fig. 1 (230, 260, 300). Disclosure p. 12-13, lines 4-13 of paragraph [0034].

[33] Fig. 1 (230, 260, 300). Disclosure end of p. 14, lines 12-15 of paragraph [0036].

[34] Fig. 1 (230, 260, 300). Disclosure end of p. 14, lines 12-15 of paragraph [0036].

[35] Fig. 1 (230, 260, 300). Disclosure end of p. 14, lines 12-15 of paragraph [0036].

[36] Fig. 1 (110). Disclosure p. 9, lines 10-11 of paragraph [0021].

[37] Fig. 1 (110). Disclosure p. 14, lines 3-11 of paragraph [0037].

[38] Fig. 1 (110). p. 14-15, lines 1-15 of paragraph [0038].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 4-11, 13-16 and 18-20 are anticipated by Ginzboorg et al. (U.S. Pat. No. 6,240,091).

Whether claims 2-3, 12 and 17 are obvious over Ginzboorg in view of Noy et al. (U.S. Pat. No. 6,539,540).

VII. ARGUMENT

A. Anticipation rejection of claims 1, 4-11, 13-16 and 18-20 over Ginzboorg

1. Claims 1, 4 and 18-20

a) The art fails to teach or suggest "a data network management system for identifying unauthorized access to a data network service…"

Independent claim 1 recites, in part, "a data network management system for identifying unauthorized access to a data network service… ." Independent claim 18 recites a similar limitation. The Examiner cites Ginzboorg at column 15, lines 40-44 as allegedly teaching the quoted limitation. However, the location cited by examiner fails to teach or suggest the quoted limitation.

Ginzboorg relates to the implementation of an access service in a telecommunications network, comprising an access network, a network that provides services, and user-operated terminals that are connected to the access network (Ginzboorg Abstract). The user terminal may generate charging messages, which if verified, give the terminal access to the network providing the services (Ginzboorg Abstract). Ginzboorg further discloses updating an access list when "the charging server sends the addresses of the terminals which currently pay for the access to the network providing the services…" and that when a "user finishes using the connection, the charging server sends a CANCEL message to the access server[, causing] the access server [to update] the access list… so that the user in question is removed from the list during the update." (Ginzboorg col. 10, ℓ. 62-col. 11, ℓ. 4). Thus, Ginzboorg's access list is a list of addresses that have paid for access to the network providing services.

Furthermore, at the location cited by the Examiner, Ginzboorg discloses that "paying customers have access to the network providing the services and the non-paying customers do not have access." In other words, non-paying or unauthorized customers "do not have access [to the network providing the services]." Since unauthorized access is expressly prohibited by Ginzboorg, Ginzboorg cannot disclose any system "for identifying unauthorized access…" as

required by the quoted limitation. None of the other art of record satisfies the deficiencies of Ginzboorg. For at least this reason, Appellants respectfully submit that the Examiner erred in rejecting independent claims 1 and 18 and all claims that depend thereon.

b) The art fails to teach or suggest "a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said service node…"

Additionally, independent claim 1 recites, in part, "a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, **said user access list specifying which users have accessed said service node**… ." Independent claim 18 recites a similar limitation. The Examiner cites Ginzboorg at column 15, lines 44-50 as allegedly teaching the quoted limitation. However, the location cited by examiner fails to teach or suggest the quoted limitation.

At the location cited by the Examiner, Ginzboorg discloses that sometimes "the router prevents the paying customers from accessing the network… or allows access for non-paying customers… [t]o correct such a situation the access server polls the router [to get the access list] and the charging server [to get the IP addresses of paying customers]." (Ginzboorg col. 15, lines 44-52). However, as discussed above, Ginzboorg's access list is a list of addresses that are permitted to access the network providing services, and is not a list of all accesses to a node or the network. Thus, the access list of G fails to teach or suggest an "access list specifying which users have accessed said service node…" as required by the quoted limitation. Furthermore, a list of IP addresses of paying customers "at the moment in question" (Ginzboorg col. 15, line 52) fails to teach or suggest an "access list specifying which users have accessed said service node… ." None of the other prior art of record satisfies the deficiencies of Ginzboorg. For at least this additional reason, Appellants

respectfully submit that the Examiner erred in rejecting independent claims 1 and 18 and all claims that depend thereon.

c) The art fails to teach or suggest "a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list..."

Additionally, independent claim 1 recites, in part, "a data processing means **for detecting unauthorized access to said service node by comparing said user access list to said authorized access list**... ." Independent claim 18 recites a similar limitation. The Examiner cites Ginzboorg at column 15, lines 50-52 as allegedly teaching the quoted limitation. However, the location cited by the Examiner fails to teach or suggest the quoted limitation.

At the location cited by the Examiner, Ginzboorg discloses comparing a list of users allowed to access the network with a list of customers who pay "at the moment in question for access to the network." (Ginzboorg col. 15, lines 50-52). Additionally, Ginzboorg discloses that the access server adds paying customers that are not included to the access list and removes included addresses that are not paying customers (Ginzboorg col. 15, lines 52-57).

Although Ginzboorg discloses a comparison of lists, it is for the purpose of updating the access list to conform to the list of paying customers at the charging server. Ginzboorg's access list does not ever keep track of accesses to the router or the network, and so there is no way to detect whether there has been an unauthorized access. Ginzboorg is merely capable of determining that an unauthorized access was possible because of the improper inclusion of an address on the access list. Thus, Ginzboorg cannot detect an unauthorized access by comparing the two lists. None of the other art of record satisfies this deficiency of Ginzboorg. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting independent claims 1 and 18 and all claims that depend thereon.

d) The art fails to teach or suggest "a data processing means... for updating said authorized access list based on the user access list retrieved from said agent"

Additionally, independent claim 1 recites, in part, "a data processing means... for updating said authorized access list based on the user access list retrieved from said agent." Independent claim 18 recites a similar limitation. The Examiner cites Ginzboorg at column 15, lines 50-52 as allegedly teaching the quoted limitation and cites Ginzboorg at column 18, lines 14-24, in reference to claims 6 and 14, as teaching a similar limitation. However, the locations cited by the Examiner fail to teach or suggest the quoted limitation.

At the location cited by the Examiner, Ginzboorg discloses "synchronization of... payments and access rights by comparing... [a] list of open connections to addresses of paying customers" and correcting any detected conflicts (Ginzboorg col. 18, lines 14-24). Thus, Ginzboorg discloses updating an access list to conform to a list of addresses of paying customers. However, Appellants' quoted limitation requires "updating said authorized access list **based on the user access list** retrieved from said agent." Appellants' "user access list" is a list of users that have accessed a particular node. Ginzboorg's disclosure of updating an access list based on a list of paying customers fails to teach or suggest updating an access list based on a list of users that have accessed a particular node. None of the other art of record satisfies this deficiency of Ginzboorg. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claims 1 and 18 and all claims that depend thereon.

Based on the foregoing, Appellants respectfully request that the rejections of claims 1 and 18 and all claims that depend thereon be reversed.

2. Claims 5-11 and 13-16

a) The art fails to teach or suggest "[a] method for identifying unauthorized access to a data network service…"

Independent claim 5 recites, in part, "[a] method for identifying unauthorized access to a data network service…" Independent claim 13 recites a similar limitation. The Examiner rejects the quoted limitation similarly to claims 1 and 18, and so for the similar portions, Appellants incorporate those remarks made with respect to claims 1 and 18. For at least this reason, Appellants respectfully submit that the Examiner erred in rejecting independent claims 5 and 13 and all claims that depend thereon.

b) The art fails to teach or suggest "determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list…"

Additionally, independent claim 5 recites, in part, "determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list… ." Independent claim 13 recites a similar limitation. The Examiner cites Ginzboorg at column 15, lines 50-52 as allegedly teaching the quoted limitation. However, the location cited by examiner fails to teach or suggest the quoted limitation.

At the location cited by the Examiner, Ginzboorg discloses comparing a list of users allowed to access the network with a list of customers who pay "at the moment in question for access to the network." (Ginzboorg col. 15, lines 50-52). Additionally, Ginzboorg discloses that the access server adds paying customers that are not included to the access list and removes included addresses that are not paying customers (Ginzboorg col. 15, lines 52-57).

Although Ginzboorg discloses a comparison of lists, it is for the purpose of updating the access list to conform to the list of paying customers at the charging server. Ginzboorg's access list does not ever keep track of accesses to the router or the network, and so there is no way to detect whether there has been an unauthorized access. Ginzboorg is merely capable of determining that

an unauthorized access was possible because of the improper inclusion of an address on the access list. Thus, Ginzboorg cannot "determine[e] if an access to said service node was unauthorized based on comparing" its two lists. None of the other art of record satisfies this deficiency of Ginzboorg. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting independent claims 5 and 13 and all claims that depend thereon.

Based on the foregoing, Appellants respectfully request that the rejections of claims 5 and 13 and all claims that depend thereon be reversed.

3. Claims 6 and 14

Dependent claim 6 recites, in part, "updating said authorized access list based on said user access list retrieved from said service node." Dependent claim 14 recites a similar limitation. Thus, Appellants respectfully submit that the Examiner erred in rejecting claims 6 and 14 for at least the reasons given above with respect to claims 1 and 18.

Based on the foregoing, Appellants respectfully request that the rejections of claims 6 and 14 be reversed.

B. Obviousness rejection of claims 2-3, 12 and 17 over Ginzboorg in view of Noy

1. Claims 2-3, 12 and 17

Claims 2-3, 12 and 17 each depend on independent claim 1, 5 or 13 and are thus allowable over Ginzboorg for the reasons given above. Furthermore, Noy fails to satisfy the above deficiencies of Ginzboorg. Thus, Appellants respectfully submit that the Examiner erred in rejecting claims 2-3, 12 and 17 for at least the reasons given above with respect to claims 1, 5 and 13.

Based on the foregoing, Appellants respectfully request that the rejections of claims 2-3, 12 and 17 be reversed.

C. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional

extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Jonathan M. Harris/

Jonathan M. Harris
PTO Reg. No. 44,144
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528-9599

VIII. CLAIMS APPENDIX

1. A data network management system for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said service node;

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node; and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.

2. The data network management system as defined in claim 1, wherein said agent is a Simple Network Management Protocol agent.

3. The data network management system as defined in claim 1, wherein said data communication means is a Simple Network Management Protocol communication means.

4. The data network management system as defined in claim 1, further including means for installing said agent at said service node, said agent having means to communicate with said data communication means.

5. A method for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, said method comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network;

b) comparing said user access list to an authorized access list;

c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list; and

d) if said access was not authorized, initiating a notification process;

wherein said user access list identifies a plurality of accesses to said service node.

6. The method as defined in claim 5, further including updating said authorized access list based on said user access list retrieved from said service node.

7. The method as defined in claim 5, further including installing said agent at said user node, prior to periodically polling and retrieving said user access list.

8. The method as defined in claim 5, further including selecting said service node for identification based on a predetermined criteria, prior to retrieving said user access list.

9. The method as defined in claim 5, wherein said notification process comprises notifying a Network Operations Console.

10. The method as defined in claim 5, wherein a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

11. The method as defined in claim 5, wherein a) through d) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

12. The method as defined in claim 5, wherein said agent is a Simple Network Management Protocol agent.

13. A computer-readable medium for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, and said medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor, cause said processor to perform steps comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in a data network;

b) comparing said user access list to an authorized access list;

c) determining if an access to said data network service was authorized based on said comparison step b);

d) if determined that said access was unauthorized, initiating a notification process.

14. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information.

15. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a).

16. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

17. The computer-readable medium as defined in claim 13, wherein said agent is a Simple Network Management Protocol agent.

18. A computer for use in a data network for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network; said computer comprising:

means for storing an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node;

a central processing unit;

data communication means for periodically polling said agent at said service node and retrieving a user access list from said agent, said user access list specifying which users have accessed said service node; and

data processing means for comparing said retrieved user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.

19. The data network as defined in claim 1, wherein said authorized access list is a common authorized user access list that includes a range of user nodes for comparing to said user access list to determine if said user access list is a subset of said common authorization access list.

20. The data network management system of claim 1 wherein said user access list identifies a plurality of accesses to said service node.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.